A Generalized Criterion for Signature Related Gröbner Basis Algorithms☆

Yao Sun and Dingkang Wang[1]

Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, CAS, Beijing 100190, China

Abstract

A generalized criterion for signature related algorithms to compute Gröbner basis is proposed in this paper. Signature related algorithms are a popular kind of algorithms for computing Gröbner basis, including the famous F5 algorithm, the extended F5 algorithm and the GVW algorithm. The main purpose of current paper is to study in theory what kind of criteria is correct in signature related algorithms and provide a generalized method to develop new criteria. For this purpose, a generalized criterion is proposed. The generalized criterion only relies on a general partial order defined on a set of polynomials. When specializing the partial order to appropriate specific orders, the generalized criterion can specialize to almost all existing criteria of signature related algorithms. For *admissible* partial orders, a complete proof for the correctness of the algorithm based on this generalized criterion is also presented. This proof has no extra requirements on the computing order of critical pairs, and is also valid for non-homogeneous polynomial systems. More importantly, the partial orders implied by existing criteria are admissible. Besides, one can also check whether a new criterion is correct in signature related algorithms or even develop new criteria by using other admissible partial orders in the generalized criterion.

Keywords: Gröbner basis, F5, signature related algorithm, generalized criterion.

1. Introduction

Gröbner basis was first proposed by Buchberger in 1965 (Buchberger, 1965). Since then, many important improvements have been made to speed up the algorithm for computing Gröbner basis (Buchberger, 1979; Lazard, 1983; Buchberger, 1985; Gebauer and Moller, 1986; Giovini et al, 1991; Mora et al, 1992; Faugère, 1999, 2002). Up to now, F5 is one of the most efficient algorithms for computing Gröbner basis. The concept of signatures for polynomials was also introduced by Faugère in (Faugère, 2002). Since F5 was proposed in

☆Version 1.2.

Email address: sunyao@amss.ac.cn, dwang@mmrc.iss.ac.cn (Yao Sun and Dingkang Wang)

[1]The authors are supported by NSFC 10971217 and 60821002/F02.

2002, it has been widely investigated and several variants of F5 have been presented, including the F5C algorithm (Eder, 2010) and F5 with extended criteria (Hashemi and Ars, 2010). Gao et al proposed an incremental algorithm G2V to compute Gröbner basis in (Gao et al, 2010a), and presented an extended version GVW in (Gao et al, 2010b).

The common characteristics of all the above algorithms are (1) each polynomial has been assigned a *signature*, and (2) both the criteria and the reduction process depend on the signatures of polynomials. The only difference among the algorithms is that their criteria are different.

By studying the criteria carefully, we find that all of these criteria work almost in a same way. Suppose f and g are polynomials with signatures and the S-pair of f and g is denoted by (t_f, f, t_g, g) where t_f and t_g are power products such that the leading power product of $t_f f$ and $t_g g$ are the same. Then a necessary condition of existing criteria to reject this S-pair is that, there exists some known polynomial h such that h's signature is a factor of $t_f f$'s or $t_g g$'s signature. However, this condition is not sufficient to make the criteria correct. Thus, existing criteria use different extra conditions to ensure correctness. With this insight, we generalize these extra conditions to a partial order defined on a set of polynomials, and then propose a generalized criterion for signature related algorithms. Therefore, when specializing the partial order to appropriate specific orders, the generalized criterion can specialize to almost all existing criteria of signature related algorithms. We emphasize that the generalized criterion can not only specialize to a *single* criterion, but also can specialize to *several* criteria at the same time. We will discuss the specializations in detail.

Unfortunately, not all general partial orders can make the generalized criterion correct. We proved that the generalized criterion is correct if the partial order is *admissible*. Unlike other proofs for the correctness of signature related algorithms (Faugère, 2002; Stegers, 2005; Eder, 2008, 2010; Hashemi and Ars, 2010; Gao et al, 2010b), the proof in this paper is complete. The proof does not need extra requirements on the computing order of critical pairs. The proof is also not limited to homogeneous polynomial systems. At present, most proofs for signature related algorithms always assume the input polynomial system is homogeneous or the critical pair with the smallest signature is computed first. However, in practical implementation, these extra requirements usually make the algorithm less efficient. Moveover, we show that the partial orders implied by the criteria of F5 and GVW are both admissible, so the proof in this paper is also valid for the correctness of F5 and GVW. A complete proof for the correctness of F5 is also given in (Sun and Wang, 2010a,b).

The significance of the generalized criterion is to show what kind of criteria for signature related algorithms is correct and provide a generalized method to check or develop new criteria. Specifically, when a new criterion is presented, if it can be specified from the generalized criterion by using an admissible partial order, then this new criterion is definitely correct. It is also possible for us to develop some new criteria by using an admissible partial order in the generalized criterion. From the proof in this paper, we know that any admissible partial order can develop a new criterion for signature related algorithms in theory, but not all of these criteria are really efficient. Therefore, we claim that if the admissible partial order is in fact a total order, then almost all useless computations can be avoided. The proof

for the claim will be included in our future works.

The paper is organized as follows. Section 2 gives the generalized criterion and describes how this generalized criterion specializes to the criteria of F5 and GVW. Section 3 proves the correctness of the generalized criterion. Section 4 discusses a new criterion by using an admissible partial order, and conducts some comparisons. Concluding remarks follow in Section 6.

2. Generalized Criterion

2.1. Generalized criterion

Let $R = \mathrm{K}[x_1, \cdots, x_n]$ be a polynomial ring over a field K with n variables. Suppose $\{f_1, \cdots, f_m\}$ is a finite subset of R. We want to compute a Gröbner basis for the ideal

$$I = \langle f_1, \cdots, f_m \rangle = \{p_1 f_1 + \cdots + p_m f_m \mid p_1, \cdots, p_m \in R\}$$

with respect to some term order on R.

Let $\mathbf{f} = (f_1, \cdots, f_m) \in R^m$, and consider the following R-module of $R^m \times R$:

$$\mathbf{M} = \{(\mathbf{u}, f) \in R^m \times R \mid \mathbf{u} \cdot \mathbf{f} = f\}.$$

Let $\mathbf{e}_i$ be the i-th unit vector of R^m, i.e. $(\mathbf{e}_i)_j = \sigma_{ij}$. Then the R-module $\mathbf{M}$ is generated by $\{(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\}$.

Fix *any* term order $\prec_1$ on R and *any* term $\prec_2$ on R^m. We must emphasize that the order $\prec_2$ may or may not be related to $\prec_1$ in theory, although $\prec_2$ is usually an extension of $\prec_1$ to R^m in implementation. For sake of convenience, we shall use the following convention for leading power products:

$$\mathrm{lpp}(f) = \mathrm{lpp}_{\prec_1}(f) \text{ and } \mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}_{\prec_2}(\mathbf{u}),$$

for any $f \in R$ and $\mathbf{u} \in R^m$. We make the convention that if $f = 0$ then $\mathrm{lpp}(f) = 0$ and $\mathrm{lpp}(f) \prec_1 t$ for any non-zero power product t in R; similarly for $\mathrm{lpp}(\mathbf{u})$. In the following, we use $\prec$ to represent $\prec_1$ and $\prec_2$, if no confusion occurs.

For any $(\mathbf{u}, f) \in \mathbf{M}$, we call $\mathrm{lpp}(\mathbf{u})$ the **signature** of $(\mathbf{u}, f)$, which is the same as the signature used in F5.

Given a finite set $B \subset \mathbf{M}$, consider a **partial order** "$\leq$" defined on B, where "$\leq$" has:

1. Reflexivity: $(\mathbf{u}, f) \leq (\mathbf{u}, f)$ for all $(\mathbf{u}, f) \in B$.
2. Antisymmetry: $(\mathbf{u}, f) \leq (\mathbf{v}, g)$ and $(\mathbf{v}, g) \leq (\mathbf{u}, f)$ imply $(\mathbf{u}, f) = (\mathbf{v}, g)$, where $(\mathbf{u}, f), (\mathbf{v}, g) \in B$.
3. Transitivity: $(\mathbf{u}, f) \leq (\mathbf{v}, g)$ and $(\mathbf{v}, g) \leq (\mathbf{w}, h)$ imply $(\mathbf{u}, f) \leq (\mathbf{w}, h)$, where $(\mathbf{u}, f)$, $(\mathbf{v}, g)$, $(\mathbf{w}, h) \in B$.

In the rest of this paper, we *do not* care about the *equality* case, so we always use "$<$", which means "$\leq$" without equality.

Based on a partial order, we give a generalized criterion for signature related algorithms.

Definition 2.1 (generalized rewritable criterion)**.** *Given a set $B \subset \mathbf{M}$ and a partial order "$<$" defined on B. We say $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in B$, f is nonzero and t is a power product in R, is* **generalized rewritable** *by B (***gen-rewritable** *for short), if there exists $(\mathbf{u}', f') \in B$ such that*

1. $\mathrm{lpp}(\mathbf{u}')$ *divides* $\mathrm{lpp}(t\mathbf{u})$*, and*
2. $(\mathbf{u}', f') < (\mathbf{u}, f)$.

In subsection 2.3, we will show how the generalized criterion specializes to some exiting criteria. In next subsection, we describe how this generalized criterion is applied.

2.2. Algorithm with generalized criterion

Let

$$G = \{(\mathbf{v}_1, g_1), \cdots, (\mathbf{v}_s, g_s)\} \subset \mathbf{M}$$

be a finite subset. We call G an **S-Gröbner basis** for $\mathbf{M}$ ("S" short for signature related), if for any $(\mathbf{u}, f) \in \mathbf{M}$, there exists $(\mathbf{v}, g) \in G$ such that

1. $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$, and
2. $\mathrm{lpp}(t\mathbf{v}) \preceq \mathrm{lpp}(\mathbf{u})$, where $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$.

If G is an S-Gröbner basis for $\mathbf{M}$, then the set $\{g \mid (\mathbf{v}, g) \in G\}$ is a Gröbner basis of the ideal $I = \langle f_1, \cdots, f_m\rangle$. The reason is that for any $f \in \langle f_1, \cdots, f_m\rangle$, there exist $p_1, \cdots, p_m \in R$ such that $f = p_1 f_1 + \cdots + p_m f_m$. Let $\mathbf{u} = (p_1, \cdots, p_m)$. Then $(\mathbf{u}, f) \in \mathbf{M}$ and hence there exists $(\mathbf{v}, g) \in G$ such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$ by the definition of S-Gröbner basis.

Suppose $(\mathbf{u}, f), (\mathbf{v}, g) \in \mathbf{M}$ are two pairs with f and g both nonzero. Let $t = \mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))$, $t_f = t/\mathrm{lpp}(f)$ and $t_g = t/\mathrm{lpp}(g)$. If $\mathrm{lpp}(t_f\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$, then

$$[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$$

is called a **critical pair** of $(\mathbf{u}, f)$ and $(\mathbf{v}, g)$. The corresponding **S-polynomial** is $t_f(\mathbf{u}, f) - ct_g(\mathbf{v}, g)$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Please keep in mind that, for any critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, we always have $\mathrm{lpp}(t_f\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$. Also notice that t_f (or t_g) here does not mean it only depends on f (or g). For convenience, we say $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is a critical pair of B, if both $(\mathbf{u}, f)$ and $(\mathbf{v}, g)$ are in B.

Given a critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, there are three possible cases, assuming $c = \mathrm{lc}(f)/\mathrm{lc}(g)$:

1. If $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) \neq \mathrm{lpp}(t_f\mathbf{u})$, then we say $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is **non-regular**.
2. If $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u})$ and $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v})$, then $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is called **super regular**.
3. If $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_g\mathbf{v})$, then we call $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ **genuine regular** or **regular** for short.

We say a **critical pair** $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ **is gen-rewritable** if *either* $t_f(\mathbf{u}, f)$ *or* $t_g(\mathbf{v}, g)$ is gen-rewritable.

We can now state the signature related Gröbner basis algorithm.

GB algorithm with generalized criterion (GBGC)
Input: $(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)$
Output: An S-Gröbner basis for $M = \langle (\mathbf{e}_1, f_1), \cdots (\mathbf{e}_m, f_m) \rangle$
begin
$G \longleftarrow \{(\mathbf{e}_i, f_i) \mid i = 1, \cdots, m\}$
$CPairs \longleftarrow \{[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)] \mid (\mathbf{u}, f), (\mathbf{v}, g) \in G\}$
$G \longleftarrow G \cup \{(f_j \mathbf{e}_i - f_i \mathbf{e}_j, 0) \mid 1 \leq i < j \leq m\}$ $(\divideontimes)$
while $CPairs \neq \emptyset$ **do**
$[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)] \longleftarrow$ **any** critical pair in $CPairs$ $(\bigstar)$
$CPairs \longleftarrow CPairs \setminus \{[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]\}$
if $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is **not gen-rewritable** by G
and $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is **regular** $(\divideontimes)$
then
$c \longleftarrow \mathrm{lc}(f)/\mathrm{lc}(g)$
$(\mathbf{w}, h) \longleftarrow$ reduce $t_f(\mathbf{u}, f) - c t_g(\mathbf{v}, g)$ by G
if $h \neq 0$,
then
$CPairs \longleftarrow CPairs \cup$ {critical pair of
$(\mathbf{w}, h)$ and $(\mathbf{w}', h') \mid (\mathbf{w}', h') \in G$ and $h' \neq 0\}$
$G \longleftarrow G \cup \{(h\mathbf{e}_i - f_i \mathbf{w}, 0) \mid i = 1, \cdots, m\}$ $(\divideontimes)$
end if
$G \longleftarrow G \cup \{(\mathbf{w}, h)\}$
end if
end while
return G
end

For the above algorithm, please notice that

1. The gen-rewritable criterion uses a partial order defined on G. While new elements are added to G, the partial order on G needs to be updated simultaneously. Fortunately, most partial orders can be updated automatically.
2. For the line ended with $(\bigstar)$, we emphasize that any critical pair can be selected, while some other algorithm, such as GVW, always select the critical pair with minimal signature.
3. The algorithm GBGC is still correct even without the lines ended with $(\divideontimes)$, but the algorithm will do some redundant computations, and hence become less efficient.
4. For sake of efficiency, it suffices to record $(\mathrm{lpp}(\mathbf{u}), f)$ for each $(\mathbf{u}, f) \in G$ in the practical implementation.

Next let us see the reduction process in the above algorithm. Given $(\mathbf{u}, f) \in \mathbf{M}$ and $B \subset \mathbf{M}$, $(\mathbf{u}, f)$ is said to be **reducible** by B, if there exists $(\mathbf{v}, g) \in B$ such that $g \neq 0$,

$\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$ and $\mathrm{lpp}(\mathbf{u}-ct\mathbf{v}) = \mathrm{lpp}(\mathbf{u})$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$ and $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$. If $(\mathbf{u}, f)$ is reducible by some $(\mathbf{v}, g) \in B$, we say $(\mathbf{u}, f)$ **reduces** to $(\mathbf{u}, f) - ct(\mathbf{v}, g) = (\mathbf{u} - ct\mathbf{v}, f - ctg)$ by $(\mathbf{v}, g)$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$ and $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$. This procedure is called a one-step reduction. Next, we can repeat this process until it is not reducible by B anymore.

There are some other ways to define the reduction process (Gao et al, 2010b; Hashemi and Ars, 2010; Faugère, 2002) and all of them have a common point. That is $\mathrm{lpp}(\mathbf{u}) = \mathrm{lpp}(\mathbf{u} - ct\mathbf{v})$, which is a key characteristic of signature related algorithms.

In the GBGC algorithm, we say a partial order "$<$" defined on G is **admissible**, if for any critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, which is regular and not gen-rewritable by G when it is being selected from *CPairs* and whose corresponding S-polynomial is reduced to $(\mathbf{w}, h)$ by G, we always have $(\mathbf{w}, h) < (\mathbf{u}, f)$ after updating "$<$" for $G \cup \{(\mathbf{w}, h)\}$. We emphasize that in the above definition of admissible, the relation $(\mathbf{w}, h) < (\mathbf{u}, f)$ is essential and $(\mathbf{w}, h)$ may not be related to other elements in G.

With the above definition, it is easy to verify whether a partial order is admissible in an algorithm. In next subsection, we will show that the partial orders implied by the criteria in F5 and GVW are admissible.

If the algorithm GBGC terminates in finite steps, then we have the following theorem.

Theorem 2.2. *Let $\mathbf{M} = \langle(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\rangle$ be an R-module in $R^m \times R$. Then an S-Gröbner basis for M can be constructed by the algorithm GBGC if the partial order in the generalized criterion is admissible.*

2.3. Specializations

In this subsection, we focus on specializing the generalized criterion to the criteria of F5 and GVW by using appropriate admissible partial orders in the algorithm GBGC.

2.3.1. Criteria of F5

First, we list the criteria in F5 by current notations. In F5, the order $\prec_2$ on R^m is obtained by extending $\prec_1$ to R^m in a POT fashion with $\mathbf{e}_1 \succ_2 \cdots \succ_2 \mathbf{e}_m$.

Definition 2.3 (syzygy criterion)**.** *Given a set $B \subset \mathbf{M}$, we say $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in B$ with $\mathrm{lpp}(\mathbf{u}) = x^\alpha \mathbf{e}_i$, f is nonzero and t is a power product in R, is* **F5-divisible** *by B, if there exists $(\mathbf{u}', f') \in B$ with $\mathrm{lpp}(\mathbf{u}') = x^\beta \mathbf{e}_j$, such that*

1. *$\mathrm{lpp}(f')$ divides tx^α, and*
2. *$\mathbf{e}_i \succ \mathbf{e}_j$.*

Definition 2.4 (rewritten criterion)**.** *Given a set $B \subset \mathbf{M}$, we say $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in B$ and t is a power product in R, is* **F5-rewritable** *by B, if there exists $(\mathbf{u}', f') \in B$ such that*

1. *$\mathrm{lpp}(\mathbf{u}')$ divides $\mathrm{lpp}(t\mathbf{u})$, and*
2. *$(\mathbf{u}', f')$ is added to B later than $(\mathbf{u}, f)$.*

In F5, given a critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ of B, if either $t_f(\mathbf{u}, f)$ or $t_g(\mathbf{v}, g)$ is F5-divisible or F5-rewritable by B, then this critical pair is redundant.

Next, we show how to specialize the generalized criterion to both syzygy criterion and rewritten criterion at the same time. For this purpose, we choose the following partial order defined on G which can be updated automatically when a new element is added to G: we say $(\mathbf{u}', f') < (\mathbf{u}, f)$ where $(\mathbf{u}', f'), (\mathbf{u}, f) \in G$, if

1. $f' = 0$ and $f \neq 0$,
2. otherwise, $(\mathbf{u}', f')$ is added to G later than $(\mathbf{u}, f)$.

The above partial order "$<$" is admissible in the algorithm GBGC. Because for any critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, which is regular and not gen-rewritable by G when it is being selected from *CPairs* and whose corresponding S-polynomial is reduced to $(\mathbf{w}, h)$ by G, the pair $(\mathbf{w}, h)$ is always added to G later than $(\mathbf{u}, f)$ no matter h is 0 or not.

At last, we show how the generalized criterion specializes to the rewritten criterion and syzygy criterion. For the rewritten criterion, the specialization is obvious by the definition of "$<$". For the syzygy criterion, if $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in G$ with $\mathrm{lpp}(\mathbf{u}) = x^\alpha \mathbf{e}_i$ and $f \neq 0$, is F5-divisible by some $(\mathbf{u}', f') \in G$ with $\mathrm{lpp}(\mathbf{u}') = x^\beta \mathbf{e}_j$, we have $\mathrm{lpp}(f')$ divides tx^α and $\mathbf{e}_i \succ \mathbf{e}_j$. According to the algorithm GBGC, since $f' \neq 0$, we have $(f'\mathbf{e}_i - f_i\mathbf{u}', 0) \in G$ and $\mathrm{lpp}(f'\mathbf{e}_i - f_i\mathbf{u}') = \mathrm{lpp}(f')\mathbf{e}_i$ divides $tx^\alpha \mathbf{e}_i$. So $t(\mathbf{u}, f)$ is gen-rewritable by $(f'\mathbf{e}_i - f_i\mathbf{u}', 0) \in G$ by definition.

With a similar discussion, the generalized criterion can also specialize to the criteria in (Hashemi and Ars, 2010), since the extended F5 algorithm in that paper only differs from the original F5 in the order $\prec_2$ on R^m.

2.3.2. Criteria of GVW

First, we rewrite the criteria in GVW by current notations.

Definition 2.5 (First Criterion)**.** *Given a set $B \subset \mathbf{M}$. We say $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in B$, f is nonzero and t is a power product in R, is* **GVW-divisible** *by B, if there exists $(\mathbf{u}', f') \in B$ such that*

1. $\mathrm{lpp}(\mathbf{u}')$ *divides* $\mathrm{lpp}(t\mathbf{u})$*, and*
2. $f' = 0$.

Definition 2.6 (Second Criterion)**.** *Given a set $B \subset \mathbf{M}$. We say $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in B$ and t is a power product in R, is* **eventually super top-reducible** *by B, if $t(\mathbf{u}, f)$ is reducible and reduced to $(\mathbf{w}, h)$ by B, and then there exists $(\mathbf{u}', f') \in B$ such that*

1. $\mathrm{lpp}(\mathbf{u}')$ *divides* $\mathrm{lpp}(\mathbf{w})$*, and*
2. $\mathrm{lpp}(f')$ *divides* $\mathrm{lpp}(h)$*, $\frac{\mathrm{lpp}(\mathbf{w})}{\mathrm{lpp}(\mathbf{u}')} = \frac{\mathrm{lpp}(h)}{\mathrm{lpp}(f')}$ and $\frac{\mathrm{lc}(\mathbf{w})}{\mathrm{lc}(\mathbf{u}')} = \frac{\mathrm{lc}(h)}{\mathrm{lc}(f')}$.*

In GVW, given a critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ of B, if $t_f(\mathbf{u}, f)$ is GVW-divisible or eventually super top-reducible by B, then this critical pair is redundant. The GVW algorithm also has a third criterion.

Third Criterion *If there are two critical pairs* $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ *and* $[\bar{t}_f(\bar{\mathbf{u}}, \bar{f}), \bar{t}_g(\bar{\mathbf{v}}, \bar{g})]$ *of* B *such that* $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(\bar{t}_f\bar{\mathbf{u}})$*, then at least one of the critical pairs is redundant.*

Next, in order to specialize the generalized criterion to the above three criteria at the same time, we use the following partial order defined on G which can also be updated automatically when a new element is added to G: we say $(\mathbf{u}', f') < (\mathbf{u}, f)$ where $(\mathbf{u}', f'), (\mathbf{u}, f) \in G$, if one of the following two conditions holds:

1. $\mathrm{lpp}(t'f') < \mathrm{lpp}(tf)$, where $t' = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{u}'))}{\mathrm{lpp}(\mathbf{u}')}$ and $t = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{u}'))}{\mathrm{lpp}(\mathbf{u})}$ such that $\mathrm{lpp}(t'\mathbf{u}') = \mathrm{lpp}(t\mathbf{u})$.
2. $\mathrm{lpp}(t'f') = \mathrm{lpp}(tf)$ and $(\mathbf{u}', f')$ is added to G later than $(\mathbf{u}, f)$.

The above partial order "$<$" is admissible in the algorithm GBGC. Because for any critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, which is regular and not gen-rewritable by G when it is being selected from *CPairs* and whose corresponding S-polynomial is reduced to $(\mathbf{w}, h)$ by G, we always have $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(\mathbf{w})$ and $\mathrm{lpp}(t_f f) > \mathrm{lpp}(h)$.

At last, let us see the three criteria of GVW.

For the first criterion, if $t(\mathbf{u}, f)$ is GVW-divisible by some $(\mathbf{u}', f') \in G$, then $t(\mathbf{u}, f)$ is also gen-rewritable by $(\mathbf{u}', f') \in G$ by definition.

For the second criterion, if $t(\mathbf{u}, f)$, where $(\mathbf{u}, f) \in G$, is eventually super top-reducible by G, then $t(\mathbf{u}, f)$ is reduced to $(\mathbf{w}, h)$ and there exists $(\mathbf{u}', f') \in G$ such that $\mathrm{lpp}(\mathbf{u}')$ divides $\mathrm{lpp}(\mathbf{w})$, $\mathrm{lpp}(f')$ divides $\mathrm{lpp}(h)$, $\frac{\mathrm{lpp}(\mathbf{w})}{\mathrm{lpp}(\mathbf{u}')} = \frac{\mathrm{lpp}(h)}{\mathrm{lpp}(f')}$ and $\frac{\mathrm{lc}(\mathbf{w})}{\mathrm{lc}(\mathbf{u}')} = \frac{\mathrm{lc}(h)}{\mathrm{lc}(f')}$. Then we have $\mathrm{lpp}(t'\mathbf{u}') = \mathrm{lpp}(\mathbf{w}) = \mathrm{lpp}(t\mathbf{u})$ and $\mathrm{lpp}(t'f') = \mathrm{lpp}(h) < \mathrm{lpp}(tf)$, which means $(\mathbf{u}', f') < (\mathbf{u}, f)$. So $t(\mathbf{u}, f)$ is gen-rewritable by $(\mathbf{u}', f') \in G$.

For the third criterion, we have $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(\bar{t}_f\bar{\mathbf{u}})$. First, if $(\mathbf{u}, f) < (\bar{\mathbf{u}}, \bar{f})$, then $\bar{t}_f(\bar{\mathbf{u}}, \bar{f})$ is gen-rewritable by $(\mathbf{u}, f)$ and hence $[\bar{t}_f(\bar{\mathbf{u}}, \bar{f}), \bar{t}_g(\bar{\mathbf{v}}, \bar{g})]$ is redundant; the reverse is also true. Second, if $(\mathbf{u}, f) = (\bar{\mathbf{u}}, \bar{f})$, one of the two critical pairs should be selected earlier from $CPairs$, assuming $[t_f(\mathbf{u}, f),\ t_g(\mathbf{v}, g)]$ is selected first. If $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is regular and not gen-rewritable, then its S-polynomial is reduced to $(\mathbf{w}, h)$ and $(\mathbf{w}, h)$ is added to G by the algorithm GBGC. Since "$<$" is admissible, we have $(\mathbf{w}, h) < (\mathbf{u}, f)$. Thus, when $[\bar{t}_f(\bar{\mathbf{u}}, \bar{f}), \bar{t}_g(\bar{\mathbf{v}}, \bar{g})]$ is selected afterwards, it will be redundant, since $\bar{t}_f(\bar{\mathbf{u}}, \bar{f})$ is gen-rewritable by $(\mathbf{w}, h)$. Otherwise, if $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is not regular, or it is regular and gen-rewritable, then $[t_f(\mathbf{u}, f),\ t_g(\mathbf{v}, g)]$ is redundant. Anyway, at least one of the critical pairs is redundant in the algorithm.

3. Proofs for the Correctness of the Generalized Criterion

To prove the main theorem (Theorem 2.2) of the paper, we need the following definition and lemmas.

In this section, we always assume that $\mathbf{M}$ is an R-module generated by $\{(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\}$. Let $(\mathbf{u}, f) \in \mathbf{M}$, we say $(\mathbf{u}, f)$ has a **standard representation** w.r.t. a set $B \subset \mathbf{M}$, if there exist $p_1, \cdots, p_s \in R$ such that

$$(\mathbf{u}, f) = p_1(\mathbf{v}_1, g_1) + \cdots + p_s(\mathbf{v}_s, g_s),$$

where $(\mathbf{v}_i, g_i) \in B$, $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(p_i\mathbf{v}_i)$ and $\mathrm{lpp}(f) \succeq \mathrm{lpp}(p_i g_i)$ for $i = 1, \cdots, s$. Clearly, if $(\mathbf{u}, f)$ has a standard representation w.r.t. B, then there exists $(\mathbf{v}, g) \in B$ such that $\mathrm{lpp}(g)$ divides $\mathrm{lpp}(f)$ and $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\mathbf{v})$ where $t = \mathrm{lpp}(f)/\mathrm{lpp}(g)$.

Lemma 3.1. *Let G be a finite set of generators for $\mathbf{M}$. Then G is an S-Gröbner basis for $\mathbf{M}$ if for any critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ of G, the S-polynomial of $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ always has a standard representation w.r.t. G.*

Proof. The proof of this lemma is direct by the theory of t-representation. For more details, please see (Becker and Weispfenning, 1993). ∎

Lemma 3.2. *Let G be a finite subset of $\mathbf{M}$ and $\{(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\} \subset G$. For an element $(\mathbf{u}, f)$ in $\mathbf{M}$, $(\mathbf{u}, f)$ has a standard representation w.r.t. G if for any critical pair $[t_g(\mathbf{v}, g), t_h(\mathbf{w}, h)]$ of G with $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t_g\mathbf{v})$, the S-polynomial of $[t_g(\mathbf{v}, g), t_h(\mathbf{w}, h)]$ always has a standard representation w.r.t. G.*

Proof. For $(\mathbf{u}, f) \in \mathbf{M}$, we have $\mathbf{u} \cdot \mathbf{f} = f$ where $\mathbf{f} = (f_1, \cdots, f_m) \in R^m$. Assume $\mathbf{u} = p_1\mathbf{e}_1 + \cdots + p_m\mathbf{e}_m$ where $p_i \in R$. Clearly, $(\mathbf{u}, f) = p_1(\mathbf{e}_1, f_1) + \cdots + p_m(\mathbf{e}_m, f_m)$. Notice that $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(p_i\mathbf{e}_i)$ for $i = 1, \cdots, m$. If $\mathrm{lpp}(f) \succeq \mathrm{lpp}(p_i f_i)$, then we have already got a standard representation for $(\mathbf{u}, f)$ w.r.t. G. Otherwise, we will prove it by the classical method. Let $T = \max\{\mathrm{lpp}(p_i f_i) \mid i = 1, \cdots, m\}$, then $T \succ \mathrm{lpp}(f)$ holds by assumption. Consider the equation

$$(\mathbf{u}, f) = \sum_{\mathrm{lpp}(p_i f_i) = T} \mathrm{lc}(p_i)\mathrm{lpp}(p_i)(\mathbf{e}_i, f_i) + \sum_{\mathrm{lpp}(p_j f_j) \prec T} p_j(\mathbf{e}_j, f_j)$$

$$+ \sum_{\mathrm{lpp}(p_i f_i) = T} (p_i - \mathrm{lc}(p_i)\mathrm{lpp}(p_i))(\mathbf{e}_i, f_i). \tag{1}$$

The leading power products in the first sum should be canceled, since we have $T \succ \mathrm{lpp}(f)$. So the first sum can be rewritten as a sum of S-polynomials, that is

$$\sum_{\mathrm{lpp}(p_i f_i) = T} \mathrm{lc}(p_i)\mathrm{lpp}(p_i)(\mathbf{e}_i, f_i) = \sum \bar{c}t(t_g(\mathbf{v}, g) - ct_h(\mathbf{w}, h)),$$

where $(\mathbf{v}, g), (\mathbf{w}, h) \in G$, $\bar{c} \in \mathrm{K}$, $t_g(\mathbf{v}, g) - ct_h(\mathbf{w}, h)$ is the S-polynomial of $[t_g(\mathbf{v}, g), t_h(\mathbf{w}, h)]$, $\mathrm{lpp}(t\ t_g g) = \mathrm{lpp}(t\ t_h h) = T$ and $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\ t_g\mathbf{v}) \succeq \mathrm{lpp}(t\ t_h\mathbf{w})$ such that we have $\mathrm{lpp}(t(t_g g - ct_h h)) \prec T$. By the hypothesis of the lemma, the S-polynomial $(t_g\mathbf{v} - ct_h\mathbf{w}, t_g g - ct_h h)$ has a standard representation w.r.t. G, that is, $(t_g\mathbf{v} - ct_h\mathbf{w}, t_g g - ct_h h) = \sum q_i(\mathbf{v}_i, g_i)$, where $(\mathbf{v}_i, g_i) \in G$, $\mathrm{lpp}(\mathbf{u}) \succeq \mathrm{lpp}(t\ t_g\mathbf{v}) \succeq \mathrm{lpp}(t\ q_i\mathbf{v}_i)$ and $\mathrm{lpp}(t_g g - ct_h h) \succeq \mathrm{lpp}(q_i g_i)$. Substituting these standard representations back to the original expression of $(\mathbf{u}, f)$ in (1), we get a new representation for $(\mathbf{u}, f)$. Let $T^{(1)}$ be the maximal leading power product of the polynomial parts appearing in the right side of the new representation. Then we have $T \succ T^{(1)}$. Repeat the above process until $T^{(s)}$ is same as $\mathrm{lpp}(f)$ for some s after finite steps. Finally, we always get a standard representation for $(\mathbf{u}, f)$. ∎

Before giving a full proof of the theorem, we introduce the following definitions first.

Suppose $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ and $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')]$ are two critical pairs, we say $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')]$ is **smaller** than $[t_f(\mathbf{u}, f),\ t_g(\mathbf{v}, g)]$ if one of the following conditions holds:

(a). $\mathrm{lpp}(t_{f'}\mathbf{u}') \prec \mathrm{lpp}(t_f\mathbf{u})$.
(b). $\mathrm{lpp}(t_{f'}\mathbf{u}') = \mathrm{lpp}(t_f\mathbf{u})$ and $(\mathbf{u}', f') < (\mathbf{u}, f)$.
(c). $\mathrm{lpp}(t_{f'}\mathbf{u}') = \mathrm{lpp}(t_f\mathbf{u})$, $(\mathbf{u}', f') = (\mathbf{u}, f)$ and $\mathrm{lpp}(t_{g'}\mathbf{v}') \prec \mathrm{lpp}(t_g\mathbf{v})$.
(d). $\mathrm{lpp}(t_{f'}\mathbf{u}') = \mathrm{lpp}(t_f\mathbf{u})$, $(\mathbf{u}', f') = (\mathbf{u}, f)$, $\mathrm{lpp}(t_{g'}\mathbf{v}') = \mathrm{lpp}(t_g\mathbf{v})$ and $(\mathbf{v}', g') < (\mathbf{v}, g)$.

Let D be a set of critical pairs. A critical pair in D is said to be **minimal** if there is no critical pair in D smaller than this critical pair. The minimal critical pair in D may not be unique, but we can always find one if D is finite.

Now, we can give the proof of the main theorem.

Proof of Theorem 2.2. If the algorithm terminates in finite steps, then G_{end} denotes the set returned by the algorithm GBGC. Since $\{(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\} \subset G_{end}$, then G_{end} is a set of generators for $\mathbf{M}$. In the rest of this proof, we focus on showing G_{end} is an S-Gröbner basis for $\mathbf{M}$.

We will take the following strategy to prove the theorem.
Step 1: Let $Todo$ be the set of *all* the critical pairs of G_{end}, and $Done$ be an empty set.
Step 2: Select a minimal critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in $Todo$.
Step 3: For such $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$, we will prove the following facts.

(F1). The S-polynomial of $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ has a standard representation w.r.t. G_{end}.
(F2). If $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *super regular* or *regular*, then $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}.

Step 4: Move $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ from $Todo$ to $Done$, i.e. $Todo \longleftarrow Todo \setminus \{[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]\}$ and $Done \longleftarrow Done \cup$
$\{[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]\}$.
We can repeat **Step 2, 3, 4** until $Todo$ is empty. Please notice that for every critical pair in $Done$, it always has property (F1). Particularly, if this critical pair is super regular or regular, then it has properties (F1) and (F2). When $Todo$ is empty, all the critical pairs of G_{end} will lie in $Done$, and hence, all the corresponding S-polynomials have standard representations w.r.t. G_{end}. Then G_{end} is an S-Gröbner basis by Lemma 3.1.

Step 1, 2, 4 are trivial, so we next focus on showing the facts in **Step 3**.

Take a minimal critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in $Todo$. And this critical pair must appear in the algorithm GBGC. Suppose such pair is selected from the set $CPairs$ in some loop of the algorithm GBGC and G_k denotes the set G at the beginning of the same loop. For such $[t_f(\mathbf{u}, f),\ t_g(\mathbf{v}, g)]$, it must be in one of the following cases:

C1: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *non-regular*.
C2: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *super regular*.
C3: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and is *not* gen-rewritable by G_k.
C4: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and $t_f(\mathbf{u}, f)$ is gen-rewritable by G_k.
C5: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and $t_g(\mathbf{v}, g)$ is gen-rewritable by G_k.

Thus, to show the facts in **Step 3**, it suffices to show (F1) holds in case **C1**, and (F1), (F2) hold in cases **C2, C3, C4** and **C5**. We will proceed for each case respectively.

We make the following claims under the condition that $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is minimal in *Todo*. The proofs of these claims will be presented later.

Claim 1: Given $(\bar{\mathbf{u}}, \bar{f}) \in \mathbf{M}$, if $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$, then $(\bar{\mathbf{u}}, \bar{f})$ has a standard representation w.r.t. G_{end}.

Claim 2: If $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is super regular or regular and $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}, then the S-polynomial of $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ has a standard representation w.r.t. G_{end}.

Claim 3: If $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is regular and $t_g(\mathbf{v}, g)$ is gen-rewritable by G_{end}, then $t_f(\mathbf{u}, f)$ is also gen-rewritable by G_{end}.

Therefore, using **Claim 2**, to show (F1) and (F2) hold in the cases **C2, C3, C4** and **C5**, it suffices to show $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end} in each case.

C1: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *non-regular*. Consider the S-polynomial $(t_f\mathbf{u} - ct_g\mathbf{v}, t_ff - ct_gg)$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Notice that $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$ by the definition of non-regular, so **Claim 1** shows $(t_f\mathbf{u} - ct_g\mathbf{v}, t_ff - ct_gg)$ has a standard representation w.r.t. G_{end}, which proves (F1).

C2: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *super regular*, i.e. $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u})$ and $\mathrm{lpp}(t_f\mathbf{u}) = \mathrm{lpp}(t_g\mathbf{v})$ where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Let $\bar{c} = \mathrm{lc}(\mathbf{u})/\mathrm{lc}(\mathbf{v})$. Notice that $\bar{c} \neq c$, since $\mathrm{lpp}(t_f\mathbf{u} - ct_g\mathbf{v}) = \mathrm{lpp}(t_f\mathbf{u})$. Then we have $\mathrm{lpp}(t_f\mathbf{u} - \bar{c}t_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$ and $\mathrm{lpp}(t_ff - \bar{c}t_gg) = \mathrm{lpp}(t_ff)$. So **Claim 1** shows $(t_f\mathbf{u} - \bar{c}t_g\mathbf{v}, t_ff - \bar{c}t_gg)$ has a standard representation w.r.t. G_{end}, and hence, there exists $(\mathbf{w}, h) \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_ff - \bar{c}t_gg) = \mathrm{lpp}(t_ff)$ and $\mathrm{lpp}(t_f\mathbf{u}) \succ \mathrm{lpp}(t_f\mathbf{u} - \bar{c}t_g\mathbf{v}) \succeq \mathrm{lpp}(t_h\mathbf{w})$ where $t_h = \mathrm{lpp}(t_ff)/\mathrm{lpp}(h)$. Consider the critical pair of $(\mathbf{u}, f)$ and $(\mathbf{w}, h)$, say $[\bar{t}_f(\mathbf{u}, f), \bar{t}_h(\mathbf{w}, h)]$. Since $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_ff)$, then $\bar{t}_f$ divides t_f, $\bar{t}_h$ divides t_h and $\frac{\mathrm{lpp}(t_f)}{\mathrm{lpp}(\bar{t}_f)} = \frac{\mathrm{lpp}(t_h)}{\mathrm{lpp}(\bar{t}_h)}$. So $[\bar{t}_f(\mathbf{u}, f), \bar{t}_h(\mathbf{w}, h)]$ is regular and smaller than $[t_f(\mathbf{u}, f),\ t_g(\mathbf{v}, g)]$ in fashion (a) or (b), which means $[\bar{t}_f(\mathbf{u}, f), \bar{t}_h(\mathbf{w}, h)]$ lies in *Done* and $\bar{t}_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}. Then $t_f(\mathbf{u}, f)$ is also gen-rewritable by G_{end}, since $\bar{t}_f$ divides t_f.

C3: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and *not* gen-rewritable by G_k. According to the algorithm GBGC, the S-polynomial $t_f(\mathbf{u}, f) - ct_g(\mathbf{v}, g)$ is reduced to $(\mathbf{w}, h)$ by G_k where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$, and $(\mathbf{w}, h)$ will be added to the set G_k afterwards. Notice that $G_k \subset G_{end}$ and $(\mathbf{w}, h) \in G_{end}$. Since "$<$" is an admissible partial order, we have $(\mathbf{w}, h) < (\mathbf{u}, f)$ by definition. Combined with the fact $\mathrm{lpp}(\mathbf{w}) = \mathrm{lpp}(t_f\mathbf{u})$, so $t_f(\mathbf{u}, f)$ is gen-rewritable by $(\mathbf{w}, h) \in G_{end}$.

C4: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and $t_f(\mathbf{u}, f)$ is gen-rewritable by G_k. Then $t_f(\mathbf{u}, f)$ is also gen-rewritable by G_{end}, since $G_k \subset G_{end}$.

C5: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is *regular* and $t_g(\mathbf{v}, g)$ is gen-rewritable by G_k. $t_g(\mathbf{v}, g)$ is also gen-rewritable by G_{end}, since $G_k \subset G_{end}$. Then **Claim 3** shows $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end} as well.

After all, the theorem is proved. ∎

We give the proofs for the three claims below.

Proof of **Claim 1**. According to the hypothesis, we have $(\bar{\mathbf{u}}, \bar{f}) \in \mathbf{M}$ and $\mathrm{lpp}(\bar{\mathbf{u}}) \prec \mathrm{lpp}(t_f\mathbf{u})$. So for any critical pair $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')]$ of G_{end} with $\mathrm{lpp}(\bar{\mathbf{u}}) \succeq \mathrm{lpp}(t_{f'}\mathbf{u}')$, we have $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')]$ is smaller than $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in fashion (a) and hence lies in *Done*, which means the S-polynomial of $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')]$ has a standard representation w.r.t. G_{end}. So Lemma 3.2 shows that $(\bar{\mathbf{u}}, \bar{f})$ has a standard representation w.r.t. G_{end}. ∎

Proof of **Claim 2**. We have that $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is minimal in $Todo$ and $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}. Let $c = \mathrm{lc}(f)/\mathrm{lc}(g)$. Then $(\bar{\mathbf{u}}, \bar{f}) = (t_f\mathbf{u} - ct_g\mathbf{v}, t_f f - ct_g g)$ is the S-polynomial of $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$. Since $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is super regular or regular, we have $\mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_f\mathbf{u})$. Next we will show that $(\bar{\mathbf{u}}, \bar{f})$ has a standard representation w.r.t. G_{end}. The proof is organized in the following way.

First: We show that there exists $(\mathbf{u}_0, f_0) \in G_{end}$ such that $t_f(\mathbf{u}, f)$ is gen-rewritable by $(\mathbf{u}_0, f_0)$ and $t_0(\mathbf{u}_0, f_0)$ is *not* gen-rewritable by G_{end} where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$.

Second: For such $(\mathbf{u}_0, f_0)$, we show that $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0 f_0)$ where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$.

Third: We prove that $(\bar{\mathbf{u}}, \bar{f})$ has a standard representation w.r.t. G_{end}.

Proof of the **First** fact. By hypothesis, suppose $t_f(\mathbf{u}, f)$ is gen-rewritable by some $(\mathbf{u}_1, f_1) \in G_{end}$, i.e. $\mathrm{lpp}(\mathbf{u}_1)$ divides $\mathrm{lpp}(t_f\mathbf{u})$ and $(\mathbf{u}_1, f_1) < (\mathbf{u}, f)$. Let $t_1 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_1)$. If $t_1(\mathbf{u}_1, f_1)$ is not gen-rewritable by G_{end}, then $(\mathbf{u}_1, f_1)$ is the one we are looking for. Otherwise, there exists $(\mathbf{u}_2, f_2) \in G_{end}$ such that $t_1(\mathbf{u}_1, f_1)$ is gen-rewritable by $(\mathbf{u}_2, f_2)$. Notice that $t_f(\mathbf{u}, f)$ is also gen-rewritable by $(\mathbf{u}_2, f_2)$ and we have $(\mathbf{u}, f) > (\mathbf{u}_1, f_1) > (\mathbf{u}_2, f_2)$. Let $t_2 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_2)$. We next discuss whether $t_2(\mathbf{u}_2, f_2)$ is gen-rewritable by G_{end}. In the better case, $(\mathbf{u}_2, f_2)$ is the needed one if $t_2(\mathbf{u}_2, f_2)$ is not gen-rewritable by G_{end}; while in the worse case, $t_2(\mathbf{u}_2, f_2)$ is gen-rewritable by some $(\mathbf{u}_3, f_3) \in G_{end}$. We can repeat the above discussions for the worse case. Finally, we will get a chain $(\mathbf{u}, f) > (\mathbf{u}_1, f_1) > (\mathbf{u}_2, f_2) > \cdots$. This chain must terminate, since G_{end} is finite and "¿" is a partial order defined on G_{end}. Suppose $(\mathbf{u}_s, f_s)$ is the last one in the above chain. Then $t_f(\mathbf{u}, f)$ is gen-rewritable by $(\mathbf{u}_s, f_s)$ and $t_s(\mathbf{u}_s, f_s)$ is not gen-rewritable by G_{end} where $t_s = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_s)$.

Proof of the **Second** fact. From the **First** fact, we have that $t_0(\mathbf{u}_0, f_0)$ is *not* gen-rewritable by G_{end} where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$. Next, we prove the **Second** fact by contradiction. Assume $\mathrm{lpp}(\bar{f}) \prec \mathrm{lpp}(t_0 f_0)$. Let $c_0 = \mathrm{lc}(\bar{\mathbf{u}})/\mathrm{lc}(\mathbf{u}_0)$. Then we have $\mathrm{lpp}(\bar{\mathbf{u}} - c_0 t_0 \mathbf{u}_0) \prec \mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_0\mathbf{u}_0)$ and $\mathrm{lpp}(\bar{f} - c_0 t_0 f_0) = \mathrm{lpp}(t_0 f_0)$. So $(\bar{\mathbf{u}} - c_0 t_0 \mathbf{u}_0, \bar{f} - c_0 t_0 f_0)$ has a standard representation w.r.t. G_{end} by **Claim 1**, and hence, there exists $(\mathbf{w}, h) \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(\bar{f} - c_0 t_0 f_0) = \mathrm{lpp}(t_0 f_0)$ and $\mathrm{lpp}(t_0\mathbf{u}_0) \succ \mathrm{lpp}(\bar{\mathbf{u}} - c_0 t_0 \mathbf{u}_0) \succeq \mathrm{lpp}(t_h\mathbf{w})$ where $t_h = \mathrm{lpp}(t_0 f_0)/\mathrm{lpp}(h)$. Next consider the critical pair of $(\mathbf{u}_0, f_0)$ and $(\mathbf{w}, h)$, say $[\bar{t}_0(\mathbf{u}_0, f_0), \bar{t}_h(\mathbf{w}, h)]$. Since $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_0 f_0)$, then $\bar{t}_0$ divides t_0, $\bar{t}_h$ divides t_h and $\frac{\mathrm{lpp}(t_0)}{\mathrm{lpp}(\bar{t}_0)} = \frac{\mathrm{lpp}(t_h)}{\mathrm{lpp}(\bar{t}_h)}$. So $[\bar{t}_0(\mathbf{u}_0, f_0), \bar{t}_h(\mathbf{w}, h)]$ is regular and smaller than $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in fashion (a) or (b), which means $[\bar{t}_0(\mathbf{u}_0, f_0), \bar{t}_h(\mathbf{w}, h)]$ lies in *Done* and $\bar{t}_0(\mathbf{u}_0, f_0)$ is gen-rewritable by G_{end}. Moreover, since $\bar{t}_0$ divides t_0, $t_0(\mathbf{u}_0, f_0)$ is also gen-rewritable by G_{end}, which contradicts with the property that $t_0(\mathbf{u}_0, f_0)$ is *not* gen-rewritable by G_{end}. The **Second** fact is proved.

Proof of the **Third** fact. According to the second fact, we have $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0 f_0)$ where $t_0 = \mathrm{lpp}(t_f\mathbf{u})/\mathrm{lpp}(\mathbf{u}_0)$. Let $c_0 = \mathrm{lc}(\bar{\mathbf{u}})/\mathrm{lc}(\mathbf{u}_0)$. We have $\mathrm{lpp}(\bar{\mathbf{u}} - c_0 t_0 \mathbf{u}_0) \prec \mathrm{lpp}(\bar{\mathbf{u}})$ and $\mathrm{lpp}(\bar{f} - c_0 t_0 f_0) \preceq \mathrm{lpp}(\bar{f})$. So $(\bar{\mathbf{u}}, \bar{f}) - c_0 t_0(\mathbf{u}_0, f_0) = (\bar{\mathbf{u}} - c_0 t_0 \mathbf{u}_0, \bar{f} - c_0 t_0 f_0)$ has a

standard representation w.r.t. G_{end} by **Claim 1**. Notice that $\mathrm{lpp}(\bar{\mathbf{u}}) = \mathrm{lpp}(t_0\mathbf{u}_0)$ and $\mathrm{lpp}(\bar{f}) \succeq \mathrm{lpp}(t_0 f_0)$. So after adding $c_0 t_0(\mathbf{u}_0, f_0)$ to both sides of the standard representation of $(\bar{\mathbf{u}}, \bar{f}) - c_0 t_0(\mathbf{u}_0, f_0)$, then we will get a standard representation of $(\bar{\mathbf{u}}, \bar{f})$ w.r.t. G_{end}.

Claim 2 is proved. ∎

Proof of **Claim 3**. Since $t_g(\mathbf{v}, g)$ is gen-rewritable by G_{end} and $\mathrm{lpp}(t_g\mathbf{v}) \prec \mathrm{lpp}(t_f\mathbf{u})$, by using a similar method in the proof of **Claim 2**, we can first show that there exists $(\mathbf{v}_0, g_0) \in G_{end}$ such that $t_g(\mathbf{v}, g)$ is gen-rewritable by $(\mathbf{v}_0, g_0)$ and $t_0(\mathbf{v}_0, g_0)$ is not gen-rewritable by G_{end} where $t_0 = \mathrm{lpp}(t_g\mathbf{v})/\mathrm{lpp}(\mathbf{v}_0)$. And then we can also prove that $\mathrm{lpp}(t_g g) \succeq \mathrm{lpp}(t_0 g_0)$ by contradiction.

If $\mathrm{lpp}(t_g g) = \mathrm{lpp}(t_0 g_0)$, then the critical pair of $(\mathbf{u}, f)$ and $(\mathbf{v}_0, g_0)$, say $[\bar{t}_f(\mathbf{u}, f), \bar{t}_0(\mathbf{v}_0, g_0)]$, must be regular and smaller than the critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in fashion (a) or (d), which means $[\bar{t}_f(\mathbf{u}, f), \bar{t}_0(\mathbf{v}_0, g_0)]$ lies in *Done* and $\bar{t}_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}. Since $\mathrm{lpp}(t_0 g_0) = \mathrm{lpp}(t_g g) = \mathrm{lpp}(t_f f)$, then $\bar{t}_f$ divides t_f, and hence, $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end} as well.

Otherwise, $\mathrm{lpp}(t_g g) \succ \mathrm{lpp}(t_0 g_0)$ holds. Let $c = \mathrm{lc}(\mathbf{v})/\mathrm{lc}(\mathbf{v}_0)$, we have $\mathrm{lpp}(t_g\mathbf{v} - c t_0\mathbf{v}_0) \prec \mathrm{lpp}(t_g\mathbf{v})$ and $\mathrm{lpp}(t_g g - c t_0 g_0) = \mathrm{lpp}(t_g g)$. Then $(t_g\mathbf{v} - c t_0\mathbf{v}_0, t_g g - c t_0 g_0)$ has a standard representation w.r.t. G_{end} by **Claim 1**, and hence, there exists $(\mathbf{w}, h) \in G_{end}$ such that $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_g g - c t_0 g_0) = \mathrm{lpp}(t_g g)$ and $\mathrm{lpp}(t_h\mathbf{w}) \preceq \mathrm{lpp}(t_g\mathbf{v} - c t_0\mathbf{v}_0) \prec \mathrm{lpp}(t_g\mathbf{v})$ where $t_h = \mathrm{lpp}(t_g g)/\mathrm{lpp}(h)$. Then the critical pair of $(\mathbf{u}, f)$ and $(\mathbf{w}, h)$, say $[\bar{t}_f(\mathbf{u}, f), \bar{t}_h(\mathbf{w}, h)]$, must be regular and smaller than the critical pair $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ in fashion (a) or (c), which means $[\bar{t}_f(\mathbf{u}, f), \bar{t}_h(\mathbf{w}, h)]$ lies in *Done* and $\bar{t}_f(\mathbf{u}, f)$ is gen-rewritable by G_{end}. Since $\mathrm{lpp}(h)$ divides $\mathrm{lpp}(t_g g) = \mathrm{lpp}(t_f f)$, then $\bar{t}_f$ divides t_f, and hence, $t_f(\mathbf{u}, f)$ is gen-rewritable by G_{end} as well.

Claim 3 is proved. ∎

4. New Criteria and comparisons

Based on the generalized criterion, to develop new criteria for signature related algorithms, it suffices to choose appropriate admissible partial orders. For example, we can develop a new criterion by using the following admissible partial order implied by GVW's criteria: that is, $(\mathbf{u}', f') < (\mathbf{u}, f)$, where $(\mathbf{u}, f), (\mathbf{u}', f') \in G$, if one of the following two conditions holds.

1. $\mathrm{lpp}(t'f') < \mathrm{lpp}(tf)$ where $t' = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{u}'))}{\mathrm{lpp}(\mathbf{u}')}$ and $t = \frac{\mathrm{lcm}(\mathrm{lpp}(\mathbf{u}),\mathrm{lpp}(\mathbf{u}'))}{\mathrm{lpp}(\mathbf{u})}$ such that $\mathrm{lpp}(t'\mathbf{u}') = \mathrm{lpp}(t\mathbf{u})$.
2. $\mathrm{lpp}(t'f') = \mathrm{lpp}(tf)$ and $(\mathbf{u}', f')$ is added to G later than $(\mathbf{u}, f)$.

We propose a new algorithm (named by NEW) based on the above criterion. This new algorithm can be considered as an improved version of GVW. We have implemented F5, GVW and NEW on Singular (version 3-1-2) with the same structure, and no special optimizations (including matrical reduction) is used such that the timing is only affected by the effect of criteria. The timings were obtained on Core i5 4×2.8 GHz with 4GB memory running Windows 7.

Another purpose of the comparison is to see the influences of computing orders of critical pairs. So we use two strategies for selecting critical pairs.

Minimal **S**ignature Strategy: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is selected from $CPairs$ if there does *not* exist $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')] \in CPairs$ such that $\mathrm{lpp}(t_{f'}\mathbf{u}') \prec \mathrm{lpp}(t_f\mathbf{u})$;

Minimal **D**egree Strategy: $[t_f(\mathbf{u}, f), t_g(\mathbf{v}, g)]$ is selected from $CPairs$ if there does *not* exist $[t_{f'}(\mathbf{u}', f'), t_{g'}(\mathbf{v}', g')] \in CPairs$ such that $\deg(\mathrm{lpp}(t_{f'}f')) \prec \deg(\mathrm{lpp}(t_f f))$.

The proof in last section ensures the algorithms, including GVW, are correct using any of the above strategies.

In the following table, we use (s) and (d) to refer the two strategies respectively. The order $\prec_1$ is graded reverse lex order and $\prec_2$ is extended from $\prec_1$ in the following way: $x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_j$, if either $\mathrm{lpp}(x^\alpha f_i) \prec_1 \mathrm{lpp}(x^\beta f_j)$, or $\mathrm{lpp}(x^\alpha f_i) = \mathrm{lpp}(x^\beta f_j)$ and $i > j$. This order $\prec_2$ has also been used in (Gao et al, 2010b; Sun and Wang, 2010b). The examples are selected from (Gao et al, 2010b).

Table 1: *#All*: number of all critical pairs generated in the computation; *#red*: number of critical pairs that are really reduced in the computation; *#gen*: number of generators in the Gröbner basis in the last iteration but before computing a reduced Gröbner basis.

	F5(s)	gvw(s)	new(s)	F5(d)	gvw(d)	new(d)
Katsura5 (22 generators in reduced Gröbner basis)						
#all	351	351	351	378	351	378
#red.	39	39	39	40	39	40
#gen.	27	27	27	28	27	28
time	1.730	1.425	1.400	1.530	1.230	1.195
Katsura6 (41)						
#all	1035	1035	1035	1225	1225	1275
#red.	73	73	73	77	77	78
#gen.	46	46	46	50	50	51
time	10.040	8.715	7.865	7.520	6.920	5.650
Katsura7 (74)						
#all	3240	3160	3160	3240	3240	3160
#red.	122	120	121	122	121	121
#gen.	81	80	80	81	81	80
time	47.840	70.371	38.750	39.440	74.535	29.950
Katsura8 (143)						
#all	12880	11325	11325	12880	11476	11325
#red.	252	242	244	252	243	244
#gen.	161	151	151	161	152	151
time	426.402	2013.28	395.844	329.390	2349.16	310.908
Cyclic5 (20)						
#all	1128	1128	1128	2211	1953	2080
#red.	56	56	56	80	76	78
#gen.	48	48	48	67	63	65
time	3.074	2.953	2.708	2.864	2.654	2.630
Cyclic6 (45)						
#all	19110	18528	18528	293761	81406	299925
#red.	234	231	231	821	463	834
#gen.	196	193	193	767	404	775
time	111.095	106.736	87.899	787.288	121.768	593.947

From the above table, we can see that the new algorithm usually has better performance than the others. There are probably two main reasons. First, the new algorithm and GVW

reject the same kind of critical pairs, but GVW's second criterion need to do some extra reductions before rejecting redundant critical pairs. Second, the critical pairs rejected by the new algorithm generally have larger leading power products than those rejected by F5 such that reductions in the new algorithm cost less time.

From the above table, we find that for some examples the algorithm with minimal signature strategy has better performance. The possible reason is that less critical pairs are generated by this strategy. For other examples, the algorithm with minimal degree strategy cost less time. The possible reason is that, although the algorithm with the minimal degree strategy usually generates more critical pairs, the critical pairs which are really needed to be reduced usually have lower degrees.

5. Conclusions and Future works

A generalized criterion for signature related algorithms is proposed in this paper. We show in detail that this generalized criterion can specialize to the criteria of F5 and GVW by using appropriate admissible orders. Moreover, we also proved that if the partial order is admissible, the generalized criterion is always correct no matter which computing order of the critical pairs is used in the algorithm. Since the generalized criterion can specialize to the criteria of F5 and GVW, the proof in this paper also ensures the correctness of F5 and GVW for any computing order of critical pairs.

The significance of this generalized criterion is to describe what kind of criterion is correct in signature related algorithms. The generalized criterion also provides a general approach to check and develop new criteria for signature related algorithms, i.e., if a new criterion can be specialized from the generalized criterion by using an admissible partial order, it must be correct; when developing new criteria, it suffices to choose admissible partial orders in the generalized criterion. We also develop a new criterion in this paper. We claim that if the admissible partial order is in fact a total order, then the generalized criterion can reject almost all useless critical pairs. The proof of the claim will be included in future works.

On the algorithm GBGC, there are several open problems.

Problem 1: Is the generalized criterion still correct if the partial order is not admissible? We do know some partial order will lead to wrong criterion. For example, consider the following partial order which is not admissible: we say $(\mathbf{u}', f') < (\mathbf{u}, f)$, where $(\mathbf{u}, f), (\mathbf{u}', f') \in G$, if $f' = 0$ and $f \neq 0$; otherwise, $(\mathbf{u}', f')$ is added to G *earlier* than $(\mathbf{u}, f)$. The above partial order leads to a wrong criterion. The reason is that $(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)$ are added to G earlier than others, so using this partial order, the generalized criterion will reject almost all critical pairs generated later, which definitely leads to a wrong output unless $\{(\mathbf{e}_1, f_1), \cdots, (\mathbf{e}_m, f_m)\}$ itself is an S-Gröbner basis. Perhaps some partial orders lead to correct criteria, and this will be studied in the future.

Problem 2: Does the algorithm GBGC always terminate in finite steps?

6. Acknowledgement

We would like to thank Shuhong Gao and Mingsheng Wang for constructive discussions.

References

T. Becker and V. Weispfenning. Gröbner bases, A Computational Approach to Commutative Algebra. Springer-Verlag. ISBN 0-387-97971-9, 1993.

B. Buchberger. Ein algorithmus zum auffinden der basiselemente des restklassenringes nach einem nulldimensionalen polynomideal. PhD thesis, Innsbruck, 1965.

B. Buchberger. A criterion for detecting unnecessary reductions in the construction of Gröbner basis. In Proc. EUROCAL 79, Lect. Notes in Comp. Sci., Springer Verlag, vol. 72, 3-21, 1979.

B. Buchberger. Gröbner bases: an algorithmic method in polynomial ideal theory. Recent trends in multidimensional system theory, N.K. bose Ed., D. Reidel Publishing Co., 184-232, 1985.

C. Eder. On the criteria of the F5 algorithm. arXiv:0804.2033v1, 2008.

C. Eder and J. Perry. F5C: a variant of Faugère's F5 algorithm with reduced Gröbner bases. Journal of Symbolic Computation, vol. 45(12), 1442-1458, 2010.

J.C. Faugère. A new efficient algorithm for computing gröbner bases (f4). Journal of Pure and Applied Algebra, vol. 139(1), 61-88, 1999.

J.C. Faugère. A new efficient algorithm for computing Grönber bases without reduction to zero (F5). In the Proceedings of ISSAC'2002, ACM Press, 75-83, 2002.

S.H. Gao, Y.H. Guan, and F. Volny. A new incremental algorithm for computing Gröbner bases. In the Proceedings of ISSAC'2010, ACM Press, Munchen, Germany, 13-19, 2010.

S.H. Gao, F. Volny, and M.S. Wang. A new algorithm for computing Gröbner bases. Cryptology ePrint Archive: Report 2010/641, 2010.

A. Hashemi and G. Ars. Extended F5 criteria. Journal of Symbolic computation, vol. 45, 1330-1340, 2010.

R. Gebauer and H.M. Moller. Buchberger's algorithm and staggered linear bases. In the Proceedings of ISSAC'1986, Waterloo, Ontario, Canada, 218-221, 1986.

A. Giovini, T. Mora, G. Niesi, L. Robbiano and C. Traverso. One sugar cube, please, or selection strategies in the Buchberger algorithm. In the Proceedings of ISSAC'1991, ACM Press, Bonn, West Germany, 49-54.

D. Lazard. Gaussian elimination and resolution of systems of algebraic equations. In Proc. EUROCAL 83, Lect. Notes in Comp. Sci., Springer Verlag, vol. 162, 146-157, 1983.

T. Mora, H.M. Möller, and C. Traverso. Gröbner bases computation using syzygies. In the Proceedings of ISSAC'1992, ACM Press, Berkeley, California, United States, 320-328, 1992.

Y. Sun and D.K. Wang. The F5 algorithm in buchberger's style. arXiv:1006.5299v2 [cs.SC]. To appear in Journal of Systems Science and Complexity, 2010.

Y. Sun and D.K. Wang. A new proof for the correctness of F5 algorithm. arXiv:1004.0084v5 [cs.SC]. Submitted to ISSAC'2011, 2010.

T. Stegers. Faugère's F5 algorithm revisited. Thesis for the degree of Diplom-Mathematiker, 2005.